REMARKS/ARGUMENTS

Request for Continued Examination:

The applicant respectfully requests continued examination of the above-indicated application as per 37 CFR 1.114.

1. Rejection of claims 1-24 under obviousness-type double patenting:

Claims 1-24 are rejected under obviousness-type double patenting as being unpatentable over claims 1-22 of US Patent 7,177,425.

Response:

Independent claims 1, 12, and 20 have been amended to clarify the present invention. Claim 1 now contains limitations previously found in dependent claims 4 and 6, claim 12 now contains limitations previously found in dependent claim 14, and claim 20 now contains limitations previously found in dependent claim 23.

As a result, each of the independent claims 1, 12, and 20 now recites that an enciphering key, which is used for enciphering access information corresponding to the communication device into the ciphertext access information, is stored in a database of a service provider that provides communication service to the communication device. The claims have also been amended to explicitly state that the enciphering key is stored outside of the communication device. Therefore, the deciphering key, which is stored in the inerasable memory, is stored in a different location than the enciphering key, which is stored outside of the phone in the database of the service provider.

One of the main features of the present invention is the additional security that comes from storing the enciphering key outside of the communication device.

The communication device only stores ciphertext access information and a deciphering key, with the enciphering key being stored in the database of the service provider. This is done to prevent an illegal user from using false access information and an enciphering key to encrypt ciphertext access information for replacing the original ciphertext access information.

This feature is explained in paragraph [0010] of the instant application, as copied below with bold text being used for emphasis on the relevant sections:

"In the present invention, an asymmetric cryptography algorithm is utilized to encipher the access information of network locks of different cell phones into ciphertext access information according to different enciphering keys. **The ciphertext access information of each cell phone is stored in each cell phone, and the corresponding deciphering key is recorded in an inerasable memory in each cell phone. The corresponding enciphering key of each cell phone is reserved in the database of the service provider only, wherein the inerasable memory is a one-time programmable memory of a lockable area in a flash memory so that the recorded deciphering key cannot be rewritten**. When a cell phone carries out network lock verification, the cell phone deciphers the ciphertext access information in the data memory into plaintext access information according to the deciphering key in the inerasable memory, and proceeds with the network lock verification according to the status of the network lock recorded in the plaintext access information. If illegal users copy ciphertext access information of another cell phone B and write it into the cell phone A attempting to break the network lock of the cell phone A, the cell phone A cannot resolve the correct plaintext access information when deciphering the ciphertext access information because **the**

deciphering keys of the cell phone A and B are different. The cell phone A can therefore determine the network lock is broken and stop the access to the communication network to prevent the security of the communication network from being violated. The access information in each cell phone is ciphertext hence illegal users are prevented from changing the access information directly to break the network lock. **Since the enciphering key is not exposed in the cell phone or in the communication network, even if illegal users are capable of falsifying the plaintext access information, the falsified plaintext access information cannot be enciphered into the correct ciphertext access information that can be deciphered by the corresponding deciphering key**."

On the other hand, the patent 7,177,425 does not teach storing the enciphering key outside of the communication device in a database of the service provider. Instead, patent 7,177,425 teaches using a single ciphering key to perform decryption and encryption. Since the ciphering key is stored in the communication apparatus, patent 7,177,425 does not teach storing an enciphering key in a database of the service provider, as claimed.

Since the patent 7,177,425 does not claim the feature of storing an enciphering key in a database of the service provider and outside of the communication device, the applicant respectfully submits that the double patenting rejection is not proper. As a result, reconsideration of claims 1-3, 5, 7-13, 15-22, and 24 is respectfully requested.

2. Rejection of claims 1-24 under 35 U.S.C. 102(f):

Claims 1-24 are rejected under 35 U.S.C. 102(f) since the applicant did not invent the claimed subject matter. See Double Patenting rejection above.

Response:

As explained above, since the patent 7,177,425 does not teach the feature of storing an enciphering key in a database of the service provider and outside of the communication device, the applicant respectfully submits that claims 1-3, 5, 7-13, 15-22, and 24 of the instant application are patentable over the patent 7,177,425. As a result, reconsideration of claims 1-3, 5, 7-13, 15-22, and 24 is respectfully requested.

3. Rejection of claims 1-24 under 35 U.S.C. 102(e):

Claims 1-24 are rejected under 35 U.S.C. 102(e) as being anticipated by Kirsch et al. (US 2005/0120225).

Response:

As explained above, independent claims 1, 12, and 20 have been amended to specify the feature of storing an enciphering key in a database of the service provider and outside of the communication device.

On the other hand, Kirsch teaches storing both a public key 70 and a private key 72 in the key data 60 area of the writable region 56 of the module memory 52. Although Kirsch teaches in paragraph [0052] that "the encrypted user data 48 may, in addition to being stored in the mobile device 10, also be transferred via the air interface 16 to a server of the ASP provider". However, Kirsch does not teach storing an enciphering key in a database of the ASP provider, and instead only teaches storing the encrypted user data 48.

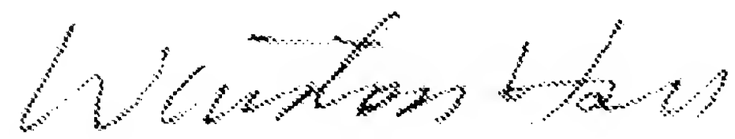
For these reasons, the applicant submits that currently amended independent claims 1, 12, and 20 are patentable over Kirsch since Kirsch does not teach all of the features of these claims.

Furthermore, claims 2, 3, 5, 7-11, 13, 15-19, 21, 22, and 24 are dependent

on claims 1, 12, and 20, and should be allowed if their respective base claims are allowed. Reconsideration of claims 1-3, 5, 7-13, 15-22, and 24 is therefore respectfully requested.

Applicant respectfully requests that a timely Notice of Allowance be issued in this case.

Sincerely yours,



Date: 07/25/2008

Winston Hsu, Patent Agent No. 41,526
P.O. BOX 506, Merrifield, VA 22116, U.S.A.
Voice Mail: 302-729-1562
Facsimile: 806-498-6673
e-mail : winstonhsu@naipo.com

Note: Please leave a message in my voice mail if you need to talk to me. (The time in D.C. is 12 hours behind the Taiwan time, i.e. 9 AM in D.C. = 9 PM in Taiwan.)